

**COMMONWEALTH OF MASSACHUSETTS  
DEPARTMENT OF TELECOMMUNICATIONS AND ENERGY**

Complaint of Global NAPs, Inc. Against	)	
Verizon for Denial of Issuance of	)	Docket No. 03-29
Collocation Access Cards	)	

**INITIAL BRIEF OF GLOBAL NAPs, INC.**

John O. Postl  
Vice President of Regulatory Affairs  
Assistant General Counsel  
89 Access Road, Suite B  
Norwood, MA 02062  
(617) 507-5121  
[jpostl@gnaps.com](mailto:jpostl@gnaps.com)

Its Attorney

May 15, 2003

## TABLE OF CONTENTS

<b>I.</b>	<b>INTRODUCTION AND SUMMARY.....</b>	<b>3</b>
<b>II.</b>	<b>VERIZON’S GUIDELINES AND APPLICABLE LAW.....</b>	<b>5</b>
	<b>A. VERIZON’S GUIDELINES.....</b>	<b>5</b>
	<b>B. FEDERAL LAW.....</b>	<b>5</b>
	<b>C. STATE LAW.....</b>	<b>7</b>
<b>III.</b>	<b>ARGUMENT.....</b>	<b>10</b>
	<b>A. VERIZON’S REQUIREMENT FOR COLLOCATORS TO PROVIDE PERSONAL INFORMATION DOES NOT SERVE LEGITIMATE SECURITY INTERESTS AND ARE UNREASONABLY INTRUSIVE INTO INDIVIDUAL’S PRIVACY RIGHTS .....</b>	<b>10</b>
	<b>B. VERIZON’ DRUG TESTING AND CHECKS DO NOT SERVE CRIMINAL BACKGROUND LEGITIMATE SECURITY INTERESTS AND VIOLATE STATE LAW .....</b>	<b>12</b>
<b>IV.</b>	<b>CONCLUSION.....</b>	<b>15</b>

**COMMONWEALTH OF MASSACHUSETTS  
DEPARTMENT OF TELECOMMUNICATIONS AND ENERGY**

Complaint of Global NAPs, Inc. Against	)	
Verizon for Denial of Issuance of	)	Docket No. 03-29
Collocation Access Cards	)	

**INITIAL BRIEF OF GLOBAL NAPs, INC.**

Global NAPs, Inc. (“Global”) respectfully submits this initial brief pursuant to the Hearing Officer Memorandum Re: Procedural Schedule; Ground Rules; and Service List dated March 25, 2003.

**I. INTRODUCTION AND SUMMARY**

“The concept of privacy embodies the ‘moral fact a person belongs to himself and not [to] others nor to society as a whole... the condition of privacy is a moral value for persons who also prize freedom and individuality; part of its defense against unwarranted invasion should include advocacy of a moral right to privacy.’”<sup>1</sup> In the wake of the September 11<sup>th</sup> attacks, the Department of Telecommunications and Energy (the “Department”) initiated an investigation of the collocation security policies of Verizon New England, Inc. *d/b/a* Verizon Massachusetts (“Verizon”)<sup>2</sup>. The Department has not, as of the date hereof, issued an Order in that docket.

As part of its new security procedures, Verizon revised its collocation access procedures. Among the changes relevant here, Verizon’s new application required

---

<sup>1</sup> Richard Sobel, *The Demeaning of Identity and Personhood in National Identification Systems*, 15 Harv. J.L. & Tech. 319, 320 (2002) (citations omitted).

collocators to provide place and date of birth, mother's maiden name and social security number. Additionally, the application requires the CLEC to provide results of its drug testing and criminal background checks. The "old" form only required a social security number. Finally, Verizon has stated that it is converting its offices to a card key system and qualified employees of collocators will be issued card keys to access Verizon offices<sup>3</sup>.

Global's employees applied for renewal of badges and access cards. Global submitted applications which did not contain the requested information and the renewal applications were denied. Global then filed the instant complaint<sup>4</sup>. Global objects to the new procedures in two material respects. First, Global believes that the provisions of personal information, such as date and place of birth and social security numbers is irrelevant to Verizon, an intrusion into the privacy of its employees and achieves no legitimate security interest. Second, requiring CLECs such as Global to undertake background checks and drug testing constitutes a barrier to entry. Global also maintains that, pursuant to applicable law, employees cannot be required to provide their social security numbers and the drug testing requirement violates state law.

Verizon answered Global's complaint stating that the Advanced Services Order permitted Verizon to establish security arrangements as long as those arrangements

---

<sup>2</sup> *Investigation by the Department of Telecommunications and Energy on its own Motion pursuant to G.L. ch. 159 §§12 and 16, into the collocation security policies of Verizon New England, Inc. d/b/a Verizon Massachusetts*, Docket No. D.T.E. 02-8.

<sup>3</sup> Verizon has stated that the "new" procedures are applicable to new employees only. Employees who currently have badges will be eligible to renew their badges using the "old" form and need not go through the drug testing or background checks.

<sup>4</sup> *Complaint of Global NAPs, Inc. Against Verizon for Denial of Issuance of Collocation Access Cards*, D.T.E. Docket No. 02-39 (filed Jan. 13, 2003).

applied equally to Verizon and all collocators<sup>5</sup>. Verizon also stated that its requirements apply equally to all collocators but to Verizon employees as well.

## **II. VERIZON'S GUIDELINES AND APPLICABLE LAW**

### **A. VERIZON'S GUIDELINES.**

Verizon's Guidelines are set forth on its website at <http://128.11.40.241/east/wholesale/resources>. The procedures that Verizon developed without consulting Global or to its knowledge any other carrier and seeks to impose on its collocators can be found there. It should be noted that Verizon's guidelines are simply that, guidelines. They do not have the force of law, nor have they been tested or challenged, except to the extent that they are being reviewed by the Department in D.T.E. 02-8 and the instant proceeding.

Global's objections to the procedures fall into two categories: first, the requirement that collocators' employees provide personal information does not serve any legitimate security interest and is unreasonably intrusive into the individual's privacy rights; and, second, the drug testing and criminal background checks do not serve legitimate security interests and violate state law.

### **B. FEDERAL LAW**

The FCC has promulgated regulations in the area of collocation as well as security. *See e.g.* 47 CFR §59.1, §59.2, §51.321, §51.323. The regulations require ILECs to make infrastructure and facilities (collocation) available to CLECs on terms and conditions that

---

<sup>5</sup> *Complaint of Global NAPs, Inc. Against Verizon for Denial of Issuance of Collocation Access Cards*, Answer of Verizon Massachusetts, D.T.E. Docket No. 02-39 (filed Jan 29, 2003).

are just, reasonable, and non-discriminatory. The ILEC must allow 24/7 unescorted access and may require the CLEC to pay for the least expensive security measures as possible. 47 CFR 51.323(h)(2)(i) identifies permissible security arrangements that may be required by the incumbent LEC *vis a vis* the collocating party, including security cameras, computerized badges, security training and use separate entrances.

The regulations cited herein identify “reasonable security measures” that involve a **LEC’s infrastructure** (*i.e.*, security cameras; separating collocated equipment). These amount to construction or facilities-related measures and are non-intrusive with respect to employees’ privacy rights. Measures contemplated by the above listed “reasonable security measures” which directly impact the employees are non-invasive, such as wearing badges or engaging in security training. While it is true that the measures suggested by section 51.323 are merely illustrative, the intention and scope of the regulations are apparent. The FCC recognized that security measures are based on the precautions that LECs must take with respect to their *premises*, not with respect to the *people* who are entering those premises. To require Global’s employees to undergo invasive measures for purported, but unspecified security reasons is unjust, unreasonable and discriminatory, in violation of 47 CFR §51.321.

### **C. STATE LAW.**

Massachusetts provides a statutory right to privacy. G. L. c. 214, §1B states “a person shall have a right against unreasonable, substantial or serious interference with his privacy. The Superior Court shall have jurisdiction and equity in one for such right and in connection therewith to award damages.”

The Massachusetts Supreme Judicial Court discussed, for the first time, private sector drug employment testing in the case of *Folmsbee v. Tech Tool Grinding & Supply, Inc.*, 417 Mass. 388, 630 N.E. 2<sup>nd</sup> 586 (1994). The court in *Folmsbee* was influenced by the fact that the company manufactured razor sharp instruments that were dangerous to handle. The court applied a balancing test which weighed the employer's interest in safety and effectiveness against the intrusion into the employee's privacy and concluded, in this case that the drug testing was appropriate. *Id.* at 393, 630 N.E. 2<sup>nd</sup> 589, 590; *see Bratt v. International Business Machines Corp.*, 392 Mass. 508, 520-521, 467 N.E. 2<sup>nd</sup> 126 (1984).

In *Webster v. Motorola, Inc.*, 418 Mass. 427 on 637 N.E. 2<sup>nd</sup> 203 (1994), the court found the employee whose position required him to drive a company-owned vehicle could be subjected to drug testing while the employee who worked as a technical editor could not, even though errors in his job could possibly result in harm to human health and safety, or to national security, the "nexus between his job duties and the harms feared is attenuated." *Webster*, at 432-434, 637 N.E. 2<sup>nd</sup> 207-208.

### **III. ARGUMENT**

#### **A. VERIZON'S REQUIREMENT FOR COLLOCATORS TO PROVIDE PERSONAL INFORMATION DOES NOT SERVE LEGITIMATE SECURITY INTERESTS AND ARE UNREASONABLY INTRUSIVE INTO INDIVIDUAL'S PRIVACY RIGHTS**

Verizon claims that its procedures are proper since it is not imposing requirements on its collocators that are more stringent than it imposes on itself. Verizon misses the point. It has not demonstrated how the measures relate to its security concerns arising from the September 11<sup>th</sup> tragedy. In fact, in discovery, Verizon has admitted that it has

never suffered a security breach which involved an individual who was under the influence of drugs or who had a felony conviction. D.T.E. 03-29 GN-VZ 1-3; 1-8. Therefore, Verizon has not demonstrated that there is even a concern that these procedures are designed to address.

When asked why Verizon requires personal information from collocator's employees, Verizon stated that the information was required to "process" applications and to permit access to collocated facilities in the case of an access card or card reader malfunction. D.T.E. 03-29 DTE-VZ 1-2. Verizon explained that by "process" it meant "reviewing the application form for completeness, comparing the application form against internal records for previous employment/cause of termination, verifying that the information provided meets the applicable criteria, gathering the necessary follow up information if the application indicates a questionable history, and manufacturing and shipping of the credentials." D.T.E. 03-29 GN-VZ 1-10. When asked specifically what purpose Verizon requires social security numbers, it replied "such information enables Verizon to cross-check its security database to determine if the applicant was involved in any prior instances of suspected or actual misconduct on Verizon's premises while employed by another carrier." D.T.E. 03-29 GN-VZ 1-11.

Two things become obvious in reviewing Verizon's own statements about its practices. First, it does not use social security numbers for any legitimate security purpose. While Verizon may choose to use social security numbers for identification purposes for its own employees (who must provide their social security numbers to Verizon for tax purposes anyway), there is no legitimate reason to force collocator employees to divulge this personal information simply because this is the system Verizon



has chosen to use. Second, Verizon has not bothered to look into the development of an alternative system which does not require the use of this personal information or who would pay for the implementation of an alternative system. *See* D.T.E. 03-29 GN-VZ 1-12. Notwithstanding that it has never occurred to Verizon to develop a system that does not rely on these numbers (many state and federal agencies such as the Massachusetts Registry of Motor Vehicles and the Federal Aviation Administration have developed alternative license numbering systems which do not require the use of social security numbers), it denies that it could possibly accomplish its security goals without this information. D.T.E. GN-VZ 1-13. Verizon's position with respect to date and place of birth information is identical. D.T.E. 03-29 GN-VZ 1-14, 1-15.

The FCC regulations governing practices refer to methods that ILECs can employ to increase security. All of the methods described above refer to making the infrastructure safer. The FCC has correctly recognized that security will be improved by making the premises more secure, not the people. The use of card key systems, video monitors and the like allow Verizon to increase security without unduly intruding into the privacy of collocators' employees.

Verizon's concerns about drug users and convicted felons are overstated, if not unfounded, and there is no legitimate security interest in requiring collocators to provide personal information. Consequently, these requirements constitute barriers to entry. In order to comply with Verizon's requirements, CLECs would have to spend additional time, money and resources to develop, implement and administer these programs. Despite its rapid growth and nationwide footprint, Global is a small company with fewer than 100 employees. Global is a family operated company and many of its employees are

related to one another by blood or marriage. The vast majority of employees have come to Global through internal referrals. D.T.E. 03-29 DTE-GN 1-4; DTE-GN 2-4; DTE-GN 2-5. Global shares in the concerns of the Department and Verizon regarding security, but at the same time, recognizes and respects the rights of its employees to protect their personal information. Forcing CLECs to implement these programs in the name of security is unfounded and while the cost of the programs might not be overwhelming, they constitute a barrier to entry nonetheless.

It is common knowledge that identity theft is on the rise world wide<sup>6</sup>. It is not unreasonable to expect that prudent people will want to protect private information to prevent credit abuse and similar identity related crime. While Verizon states that it does not use the information contained in its application for any purpose other than security, the risk exists that this information could be used for improper purposes. The Department should weigh the interests of Verizon in using a social security number based system, designed for its convenience, with the legitimate privacy interests of the collocators' employees who are forced to give away personal information in order to remain employed.

**B. VERIZON'S DRUG TESTING AND CRIMINAL BACKGROUND CHECKS DO NOT SERVE LEGITIMATE SECURITY INTERESTS AND VIOLATE STATE LAW**

Verizon's drug testing program violates the Massachusetts Civil Rights Act and the right to privacy, under G. L. c. 214, §1B, because Verizon has no reason to believe that CLEC's employees are impaired by drugs or that the health and safety of CLEC's and Verizon's employees, or the safety of its equipment, are in jeopardy or at immediate

risk. Verizon's purported justification for these additional security measures was the September 11<sup>th</sup> tragedy, but it fails to articulate how these measures directly address the threat posed by increased terrorist activity.

Further, because CLEC's employees will be utilizing Global's vehicles to travel to Verizon's premises to service or maintain CLEC's equipment, Verizon's purported security concerns are difficult to identify, which diminishes the alleged risk to its interests. Perhaps if CLEC employees were operating Verizon vehicles, it could arguably establish a nexus between the activity and the harm under *Webster*, but here, those fears are unfounded.

Because the relationship between CLECs and Verizon is contractual and since CLEC employees must have access to Verizon sites in order to do their jobs, Verizon cannot force CLECs to violate the constitutional and statutory rights of their employees under the guise of unidentified security concerns. Verizon's practices put CLECs at risk for potential claims from their employees.

Even Verizon's "national security" concerns are insufficient to justify the drug testing program. The *Folmsbee* and *Webster* cases illustrate that courts will engage in a detailed factual analysis of both the employer's type of business and the specific duties performed by employees to be tested. The lack of any existing security problems with CLECs' employees; the nature of the employees' positions coupled with the fact that they operate CLECs' equipment; and the existence of on-site security measures at Verizon's premises serve to erode Verizon's purported justification for its intrusive measures. Additionally, 47 CFR §51.323(h)(2)(i) specifically addresses and identifies the reasonable

---

<sup>6</sup> See Nicole M. Buba, *Waging War Against Identity Theft: Should the United States Borrow from the European Union's Battallion?*, 23 Suffolk Transnat'l L. Rev. 633, 634

security measures that the incumbent LEC may adopt. Since none of the measures listed include drug or alcohol testing programs, or other measures invasive with respect to an employee's privacy interest, the intention of the regulations was to focus on infrastructure security measures and employee training. If drug/alcohol screening or criminal background investigations were intended, then Congress would have included these measures. Since the Department has treated this as a "law" case, and the parties have presented no testimony and there have been no evidentiary hearings, the Department cannot engage in the balancing test set forth above.

#### **IV. CONCLUSION**

For the foregoing reasons, the Department should not require collocators to implement drug testing or criminal background checks for its employees since these have no legitimate purpose in advancing Verizon's security concerns. The Department should also not require collocators' employees to provide their date and place of birth and their social security numbers, rather, the Department should order Verizon to implement a system which does not require collocators' to provide this intrusive level of information. Finally, the Department should order Verizon to bear the costs of the new system since it was Verizon's decision to unnecessarily invade the privacy of its collocator's employees.

Respectfully submitted,

GLOBAL NAPS, INC.

---

John O. Postl  
Vice President of Regulatory Affairs  
Assistant General Counsel  
89 Access Road, Suite B  
Norwood, MA 02062  
(617) 507-5121  
[jpostl@gnaps.com](mailto:jpostl@gnaps.com)

Its Attorney